BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: **13**/BC-CATTT

Hà Nội, ngày 27 tháng 03 năm 2018

TÓM TẮT
Tình hình an toàn thông tin đáng chú ý trong tuần 12/2018 (từ ngày 19/3/2018 đến ngày 25/3/2018)

BẢNG TỔNG HỢP

1. Nhằm cải thiện việc kết nối với cử tri cũng như tăng cường thêm các công cụ, nâng cao khả năng phòng, chống tấn công mạng để bảo vệ hệ thống bầu cử, Chính phủ Hoa Kỳ thành lập Trung tâm phân tích và chia sẻ thông tin cơ sở hạ tầng bầu cử.

2. NIST đang cho đăng công khai để lấy ý kiến rộng rãi đến hết ngày 18/5/2018 đối với dự thảo tiêu chuẩn cung cấp hướng dẫn cho các tổ chức hạn chế nguy cơ mất an toàn thông tin và phục hồi hệ thống do các cuộc tấn công mạng, đặc biệt là các cuộc tấn công APT.

3. Trong tuần, Cục ATTT ghi nhận có ít nhất 51 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc; lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động.

1. Điểm tin đáng chú ý

1.1. Nhằm cải thiện việc kết nối với cử tri cũng như tăng cường thêm các công cụ, nâng cao khả năng phòng, chống tấn công mạng để bảo vệ hệ thống bầu cử, Chính phủ Hoa Kỳ thành lập Trung tâm phân tích và chia sẻ thông tin cơ sở hạ tầng bầu cử (The Elections Infrastructure Information Sharing and Analysis Center - ISAC).

ISAC giúp các địa phương giải quyết những vấn đề liên quan tới chia sẻ thông tin các cuộc tấn công mạng, lỗ hổng và giám sát an toàn thông tin từ xa. Trung tâm An toàn Internet (CIS - Center for Internet Security) được giao nhiệm vụ thành lập và điều hành ISAC. Hệ thống chia sẻ thông tin các bang (Multi-

State ISAC) sẽ được sử dụng để chia sẻ thông tin, điều hành, hợp tác về an toàn trong bầu cử nhằm thay thế cho các văn phòng chính thức.

Trước đó, Chính phủ Hoa Kỳ cũng đã xây dựng các hệ thống chia sẻ thông tin tương tự cho những lĩnh vực cơ sở hạ tầng quan trọng như: lĩnh vực tài chính, ngành điện và ngành hàng không.

1.2. NIST công bố dự thảo tiêu chuẩn "Kỹ thuật an toàn hệ thống: Các biện pháp phục hồi kỹ thuật cho các hệ thống mạng an toàn tin cậy". Dự thảo tiêu chuẩn cung cấp hướng dẫn nhằm giúp các tổ chức hạn chế nguy cơ mất an toàn thông tin và phục hồi hệ thống do các cuộc tấn công mạng, đặc biệt là các cuộc tấn công APT.

Theo NIST, dự thảo tiêu chuẩn này có thể được xem như một cuốn cẩm nang để các tổ chức có thể sử dụng một phần hoặc tất cả các nguyên tắc về khả năng phục hồi trên không gian mạng được mô tả và áp dụng cho các môi trường kỹ thuật, vận hành. Để giúp các tổ chức xây dựng khả năng phục hồi trên không gian mạng của hệ thống, dự thảo này bao gồm các phần về thực hiện, tích hợp, xác minh, chuyển đổi, xác nhận, vận hành, duy trì và xử lý.

NIST đang cho đăng công khai dự thảo tiêu chuẩn này để lấy ý kiến rộng rãi đến hết ngày 18/5/2018.

1.3. Đầu tháng 3 năm 2018, theo thông tin từ Microsoft, hãng này đã phát hiện một cuộc tấn công mã độc đào tiền ảo lây nhiễm gần 500.000 máy tính chỉ trong vòng 12 tiếng và ngăn chặn thành công việc mã độc này lây lan rộng hơn.

Theo bài nghiên cứu, mã độc được gọi là Dofoil (hay còn được gọi là Smoke Loader) lây nhiễm vào các máy tính sử dụng hệ điều hành Windows và lợi dụng hiệu năng CPU của các máy bị nhiễm để đào tiền ảo Electroneum. Dofoil sử dụng một kỹ thuật chèn mã cũ được gọi là “làm rỗng tiến trình”, tạo ra một tiến trình mới có chứa mã độc hại của tiến trình hợp lệ và thực thi mã độc thay vì tiến trình gốc, điều này khiến các công cụ giám sát tiến trình và phần mềm chống mã độc khó phát hiện ra nó.

Theo mẫu mã độc mà Microsoft nghiên cứu, tiến trình explorer.exe sẽ tạo một bản sao của mã độc trong thư mục Roaming AppData và đổi tên nó thành ditereah.exe, sau đó nó sẽ tạo một khóa registry OneDrive Run và trỏ tới bản sao mã độc vừa tạo.

Người dùng cuối có thể sử dụng phần mềm phòng, chống mã độc Windows Defender Antivirus (có sẵn trên hệ điều hành Windows hoặc tải và cài

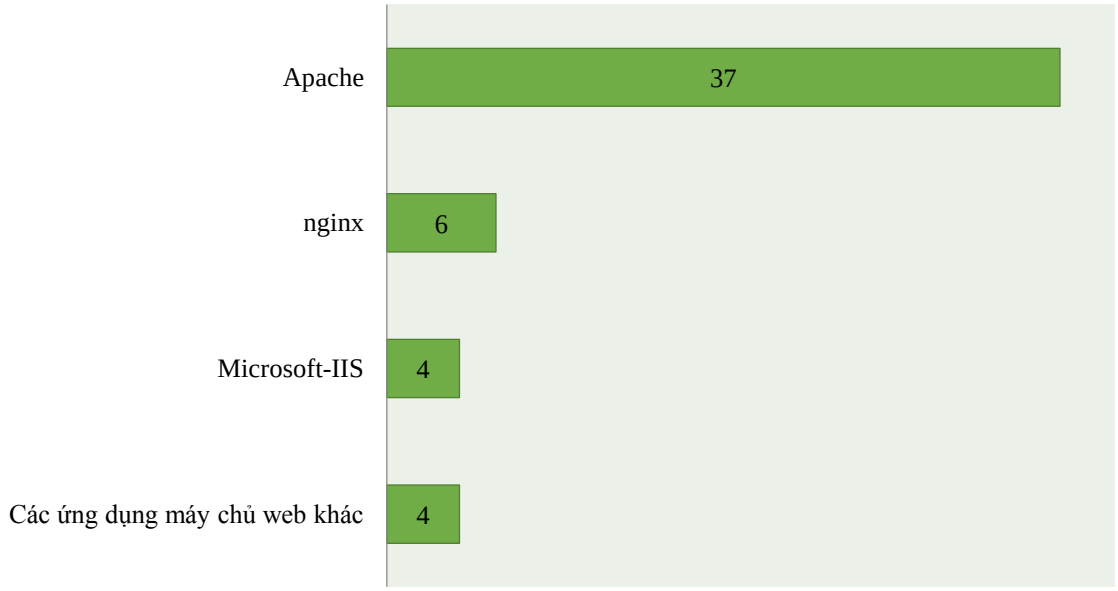
đặt từ trang web của Microsoft) để tự động loại bỏ mã độc Dofoil khi chúng khởi chạy. Tuy nhiên, việc nhiễm mã độc trước đó có thể để lại các tập tin bị lây nhiễm và thay đổi hệ thống vì vậy người dùng cần cập nhật Windows Defender Antivirus và quét lại toàn bộ hệ thống để giải quyết vấn đề này.

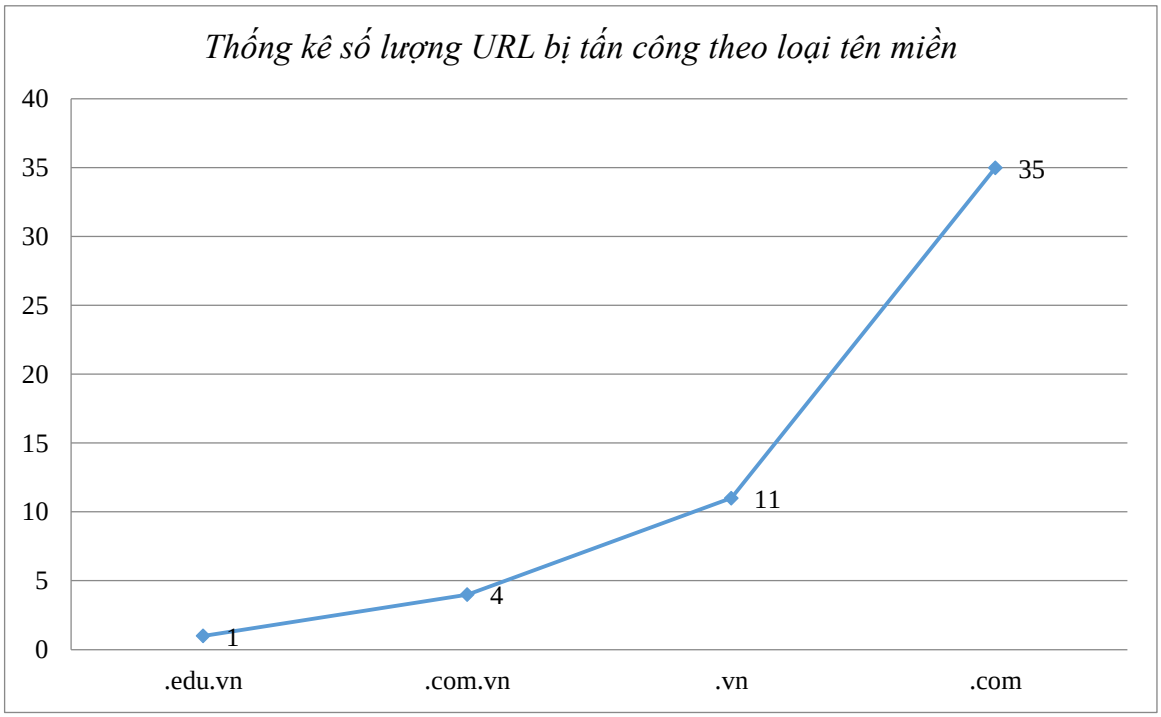
2. Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam

Qua theo dõi, trích xuất thông tin từ hệ thống kỹ thuật thời gian qua, Cục ATTT nhận thấy trên không gian mạng đang tồn tại nhiều trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin như: phát tán thư rác; tấn công từ chối dịch vụ; cài đặt và phát tán các loại mã độc (gần đây nhất là cài đặt và phát tán mã độc để đào tiền ảo); lưu trữ các mã khai thác điểm yếu lỗ hổng một cách tự động (như lỗ hổng trên trình duyệt hay các thành phần mở rộng của trình duyệt mà người dùng sử dụng .v.v…).

Trong tuần, Cục ATTT ghi nhận có ít nhất 51 đường dẫn (URL) trên các trang web tại Việt Nam bị tấn công, lợi dụng để thực hiện các hành vi gây mất an toàn thông tin. Trong đó, thống kê, phân loại các đường dẫn này theo loại ứng dụng máy chủ web (IIS, Apache …) và loại tên miền (.com, .vn, …) cụ thể như sau:

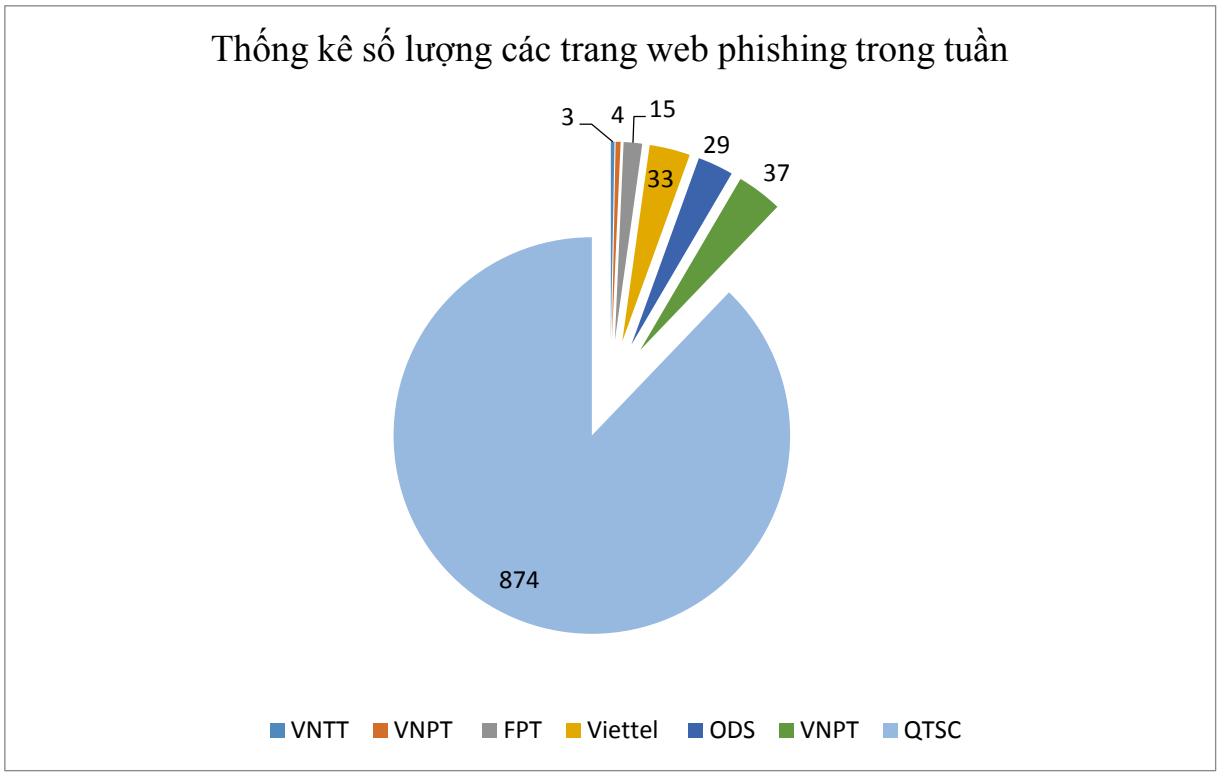
Thống kê số lượng URL bị tấn công theo ứng dụng máy chủ web



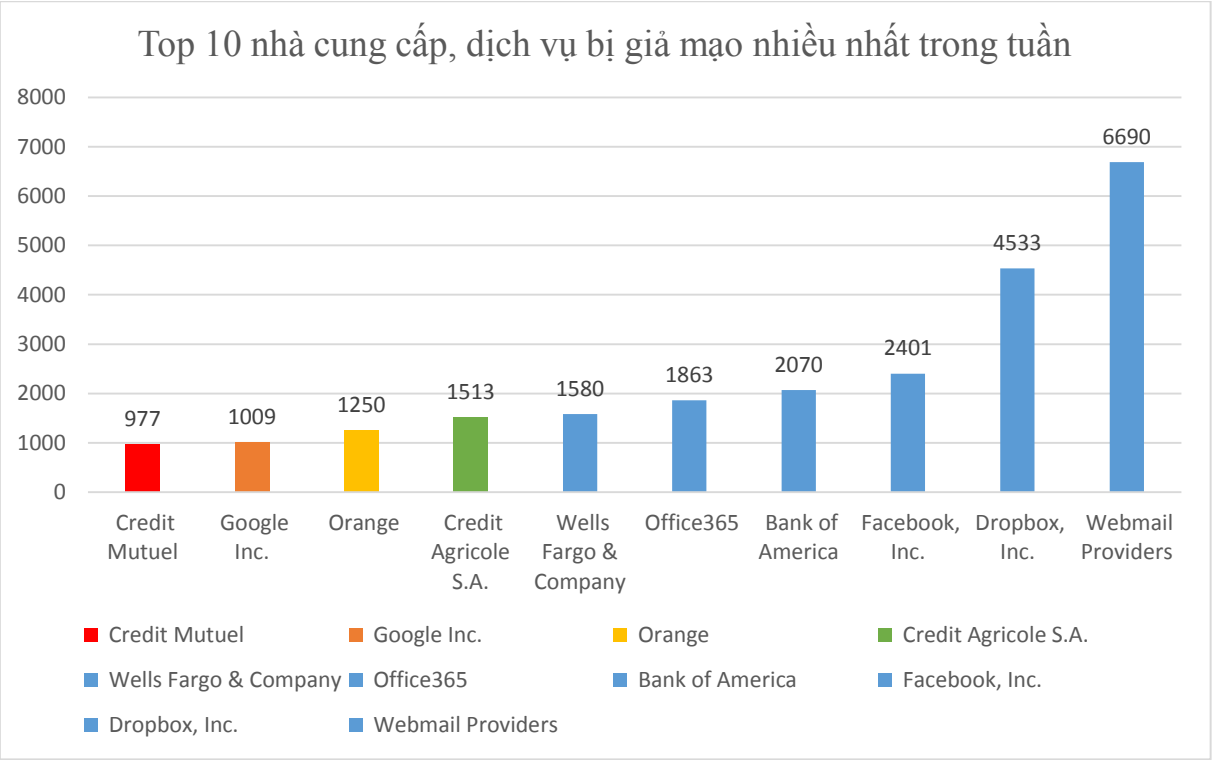


3. Tình hình tấn công lừa đảo (Phishing) trong tuần

3.1. Qua thu thập, theo dõi, trích xuất từ hệ thống kỹ thuật, Cục ATTT còn ghi nhận có ít nhất 995 trang web đặt tại Việt Nam bị lợi dụng để thực hiện tấn công Phishing trong tuần.



3.2. Trên thế giới có nhiều các trang web giả mạo các tổ chức, doanh nghiệp, nhà cung cấp, dịch vụ lớn như Facebook, PayPal, Dropbox .v.v…



Việt Nam có nhiều người dùng các dịch vụ, ứng dụng nước ngoài (cả miễn phí và có phí) như Facebook, Dropbox .v.v… vì vậy người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản.

4. Lỗ hổng/điểm yếu an toàn thông tin trong tuần

4.1. Trong tuần, các tổ chức quốc tế đã phát hiện và công bố ít nhất 274 lỗ hổng trong đó có: 15 lỗ hổng RCE (cho phép chèn và thực thi mã lệnh), 03 lỗ hổng đã có mã khai thác.

4.2. Hệ thống kỹ thuật của Cục An toàn thông tin chủ động rà quét trên không gian mạng Việt Nam, đánh giá, thống kê cho thấy có **06** nhóm lỗ hổng trên các sản phẩm, dịch vụ CNTT phổ biến, có thể gây ảnh hưởng lớn đến người dùng ở Việt Nam, như: nhóm 20 lỗ hổng trên một số sản phẩm, ứng dụng của IBM; Nhóm 08 lỗ hổng trên các sản phẩm, hệ điều hành của Huawei .v.v

4.3. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	AMD	CVE-2018-8934 CVE-2018-8935 CVE-2018-8932	Nhóm 07 lỗ hổng bảo mật trên bộ xử lý AMD của một số nền tảng như EPYC, Ryzen, Ryzen Pro và Ryzen Mobile cho phép tấn công leo thang, đặc biệt phát	AMD đang làm việc với các hãng để đưa ra

			hiện một số backdoor có sẵn trong firmware. Cục ATTT đang tiếp tục theo dõi nhóm lỗ hổng này.	bản vá
2	Dell	CVE-2018-1211 CVE-2018-1218 CVE-2018-1207	Nhóm 03 lỗ hổng trên một số sản phẩm, dịch vụ của Dell (Dell EMC iDRAC7/iDRAC8, Dell EMC NetWorker) cho phép thực hiện tấn công từ chối dịch vụ, tấn công Path Traversal, đặc biệt lỗ hổng CVE-2018-1207 cho phép chèn và thực thi mã lệnh.	Đã có thông tin xác nhận và bản vá.
3	F5	CVE-2018-5504 CVE-2018-5502 CVE-2018-5505	Nhóm 06 lỗ hổng trên một số sản phẩm ứng dụng của F5 (BIG-IP nhiều phiên bản) cho phép thực hiện tấn công từ chối dịch vụ, chèn và thực thi mã lệnh,	Đã có xác nhận và thông tin bản vá.
4	Huawei	CVE-2017-8187 CVE-2017-17215 CVE-2017-8176 CVE-2017-15326 CVE-2017-17306 …..	Nhóm 08 lỗ hổng trên một số dòng sản phẩm của Huawei (FusionSphere OpenStack, HG532, Huawei IPTV STB, và một số dòng điện thoại) cho phép chèn và thực thi mã lệnh	Đã có thông tin xác nhận và bản vá.
5	IBM	CVE-2017-1677 CVE-2018-1448 CVE-2018-1427 CVE-2015-7458 CVE-2017-1655	Nhóm 20 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (Data Server Driver, DB2, GSKit, IBM Connections, IBM Jazz Foundation) cho phép thực hiện nhiều hình thức tấn công khác nhau gồm tấn công XSS, thu thập thông tin, nhiều lỗ hổng cho phép chèn và thực thi mã lệnh	Đã có thông tin xác nhận và bản vá.

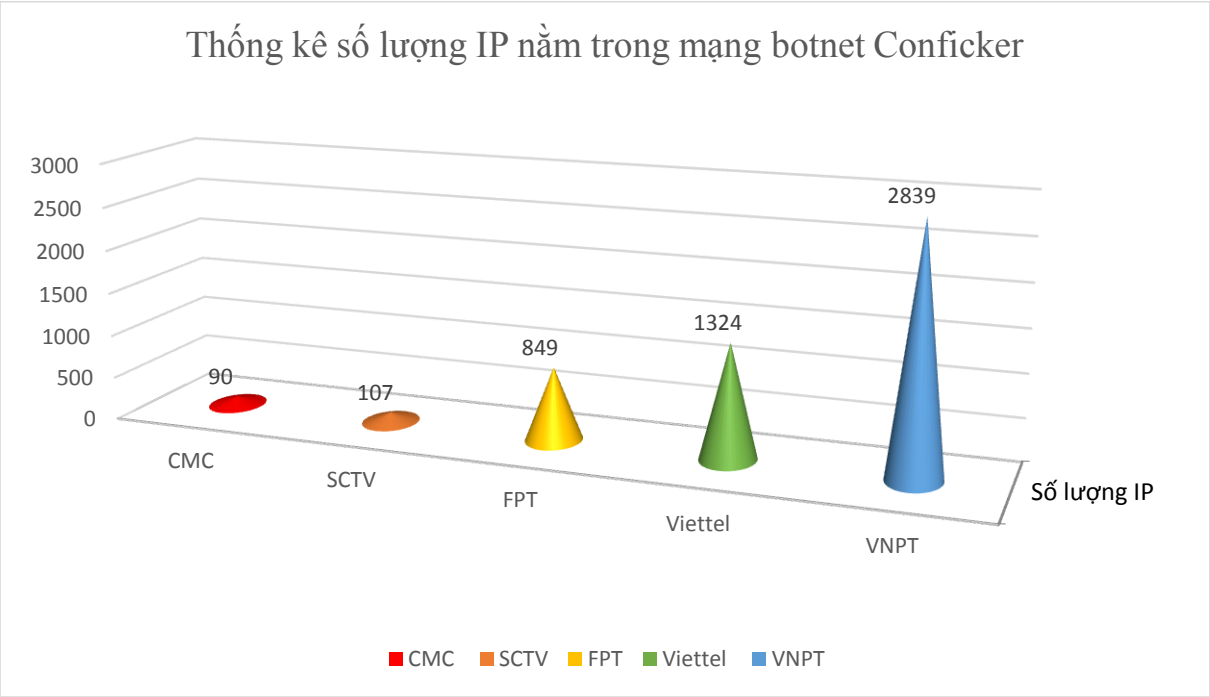
6	Tenda	CVE-2018-5768 CVE-2018-5770	Nhóm 02 lỗ hổng trên thiết bị router Tenda AC 15 cho phép đối tượng tấn công có thể thực thi mã lệnh và kiểm soát thiết bị.	Chưa có thông tin xác nhận và bản vá.

5. Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam

5.1. Mạng botnet Conficker

Mạng botnet Conficker được phát hiện từ tháng 10/2008. Mã độc này được thiết kế nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác. Những máy tính bị lây nhiễm đều không truy cập được các website liên quan đến phần mềm diệt virus hay dịch vụ cập nhật của hệ Windows (Windows Update).

Mặc dù mạng botnet Conficker xuất hiện từ năm 2008, lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật, tuy nhiên tại Việt Nam, số lượng máy tính nằm trong mạng botnet Conficker vẫn còn rất nhiều trong tuần mà Cục An toàn thông tin đang theo dõi.



5.2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

TT	Tên miền/IP
1	g.omlao.com
2	u.amobisc.com
3	i.onaoy.com
4	mk.omkol.com
5	jwd0ylsp.ru
6	4yuwi9kbmm.ru
7	kukutrustnet777.info
8	qhcqvdmp.ru
9	104.244.14.252
10	09wb2knotg.ru

6. Khuyến nghị đối với các cơ quan, đơn vị

Nhằm bảo đảm an toàn thông tin trong hệ thống mạng của các cơ quan, tổ chức, Cục An toàn thông tin khuyến nghị:

- Nhằm tránh việc bị các đối tượng tấn công lợi dụng các trang web để thực hiện các hành vi gây mất an toàn thông tin như đã nêu trong *mục 2*, các cơ quan tổ chức cần phải thường xuyên kiểm tra, rà soát máy chủ web để kịp thời phát hiện và cập nhật các điểm yếu, lỗ hổng trên các máy chủ web thuộc cơ quan, tổ chức mình

- Người dùng cần phải hết sức cảnh giác với những trang web giả mạo để ăn trộm tài khoản, đặc biệt là các trang web giả mạo các ứng dụng, dịch vụ phổ biến như đã nêu trong *mục 3.2* báo cáo này.

- Theo dõi và cập nhật bản vá cho các lỗ hổng, đặc biệt là lỗ hổng nêu tại *mục 4.3* báo cáo này.

- Chủ động kiểm tra, rà soát, bóc gỡ mã độc ra khỏi hệ thống mạng. Cục An toàn sẵn sàng phối hợp với các cơ quan tổ chức tiến hành kiểm tra và bóc gỡ mã độc botnet trên hệ thống của cơ quan đơn vị. Để xác minh các máy tính bị nhiễm mã độc botnet, Quý đơn vị có thể liên hệ với Cục An toàn thông tin theo thông tin bên dưới để phối hợp thực hiện.

- Kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiệu kết nối đến các tên miền độc hại Cục An toàn thông tin đã chia sẻ, đặc biệt là các tên miền đã nêu trong *mục 5.2* báo cáo này.

Thông tin liên hệ Cục An toàn thông tin, tầng 8, số 115 Trần Duy Hưng, quận Cầu Giấy, TP. Hà Nội; số điện thoại: 024.3943.6684; thư điện tử ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Bộ trưởng và các Thứ trưởng (để b/c);
- Thư ký Lãnh đạo Bộ;
- Đơn vị chuyên trách về CNTT các bộ, ngành;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Cục KSTTHC, Văn phòng Chính phủ;
- Vụ Khoa giáo - Văn xã, Văn phòng Chính phủ;
- Trung tâm CNTT, Văn phòng Trung ương Đảng;
- Trung tâm CNTT, Văn phòng Quốc Hội; (email)
- Trung tâm CNTT, Văn phòng Chủ tịch nước;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và Ngân hàng;
- Cơ quan, đơn vị thuộc Bộ;
- Lãnh đạo Cục;
- Lưu: VT, TTTV.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Huy Dũng

PHỤ LỤC

I. Báo cáo được xây dựng dựa trên các nguồn thông tin:

- Hệ thống xử lý tấn công mạng Internet Việt Nam, hệ thống trang thiết bị kỹ thuật phục vụ cho công tác quản lý nhà nước về an toàn thông tin do Cục An toàn thông tin quản lý vận hành;

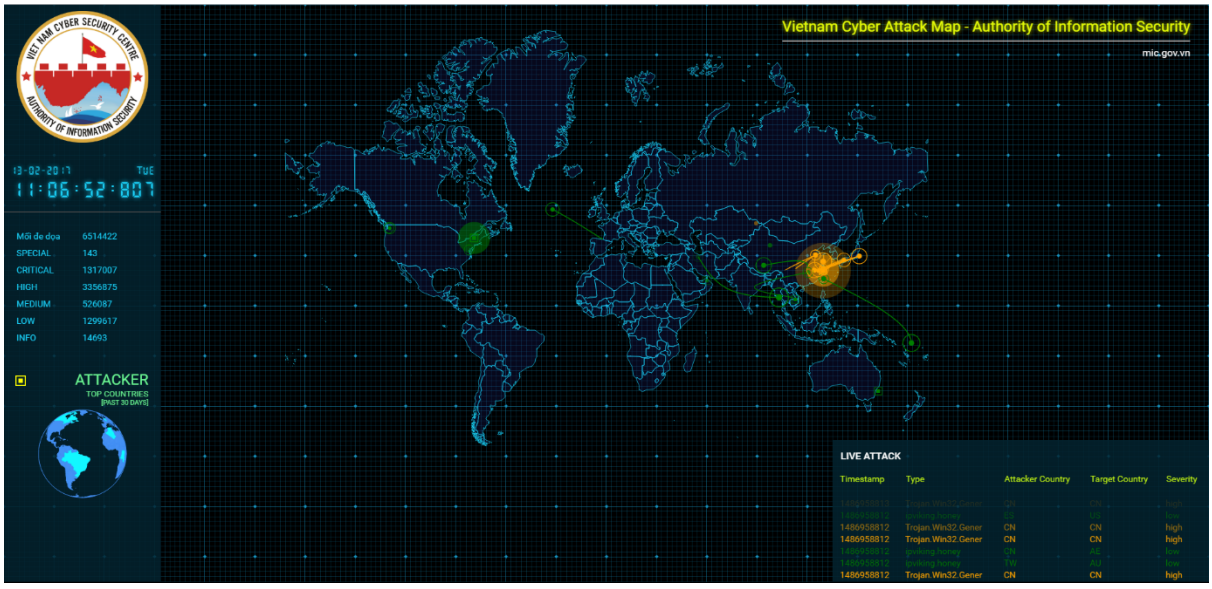
- Kênh liên lạc quốc tế về an toàn thông tin; hoạt động hợp tác giữa Cục An toàn thông tin và các tổ chức, hãng bảo mật trên thế giới.

- Hoạt động theo dõi, phân tích, tổng hợp tình hình an toàn thông tin mạng trên các trang mạng uy tín.

II. Giới thiệu về Hệ thống theo dõi, xử lý tấn công mạng Internet Việt Nam trực thuộc Cục An toàn thông tin:

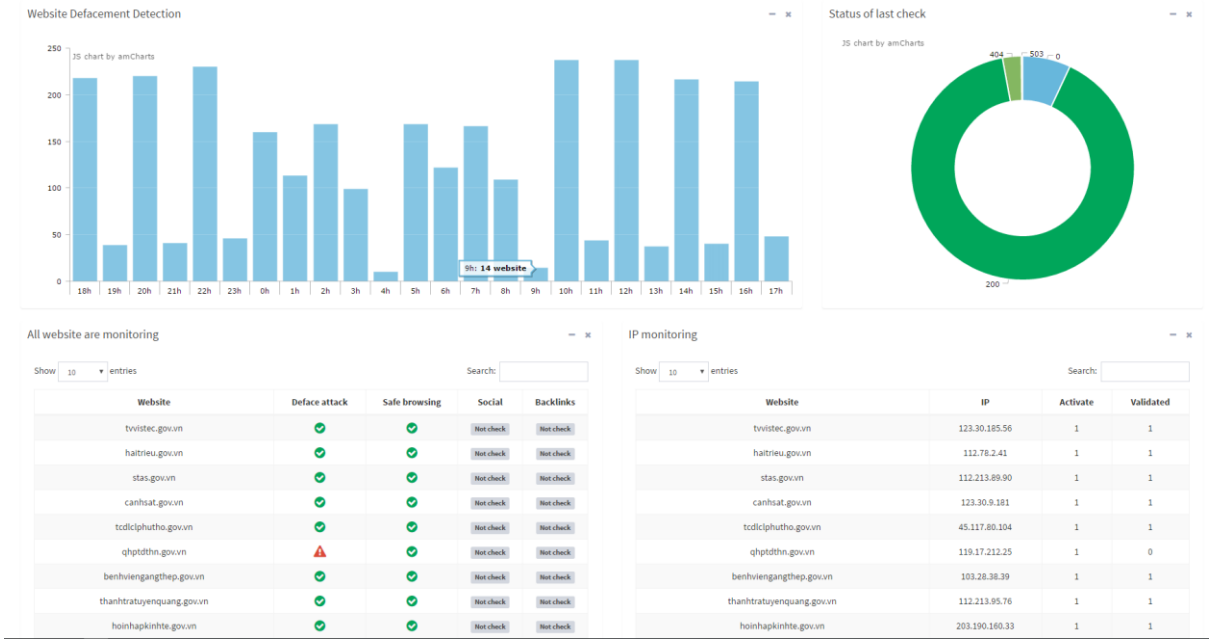
Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT trực thuộc Cục An toàn thông đang triển khai và vận hành các hệ thống kỹ thuật phục vụ công tác bảo đảm ATTT mạng quốc gia như sau:

1. Hệ thống phân tích, phát hiện tấn công mạng từ xa đa nền tảng



Hệ thống được xây dựng dựa trên các công nghệ AI, thường xuyên dò quét, kiểm tra các mục tiêu dựa trên hệ thống sensor sẵn có của Cục An toàn thông tin và các sensor khác trên toàn thế giới, từ đó, tự động phát hiện, cảnh báo sớm các cuộc tấn công mạng nhắm vào các mục tiêu được cấu hình sẵn, nhanh chóng thông báo cho quản trị viên biết các tình trạng của các cuộc tấn công mạng này.

2. Hệ thống phân tích, dò quét, tự động phát hiện tấn công từ xa các website, cổng thông tin điện tử



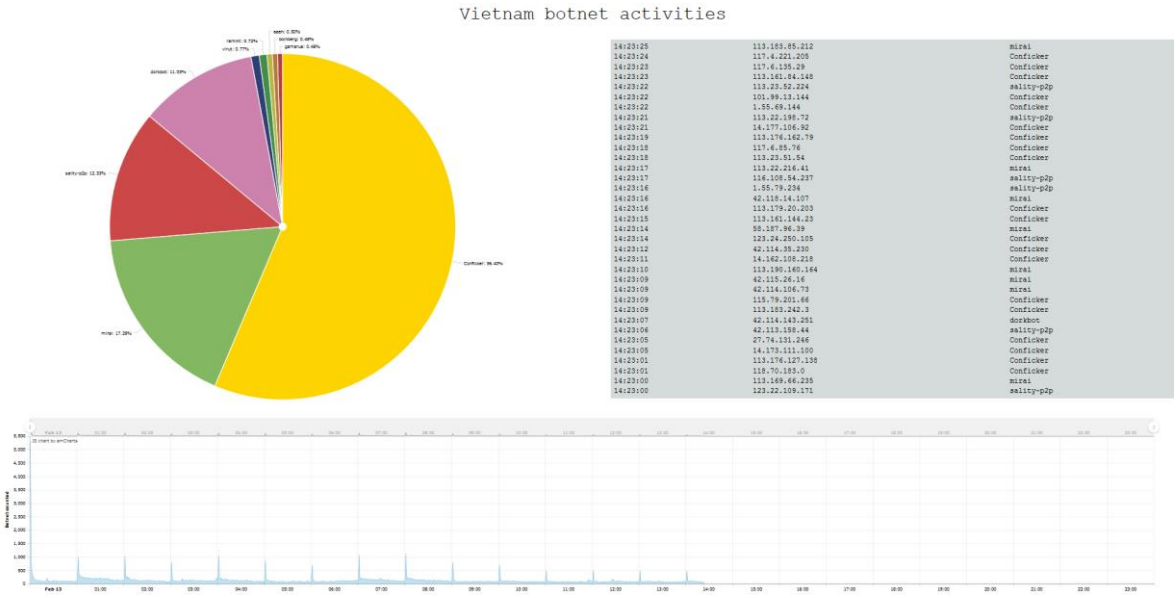
Trước tình hình các hệ thống website, trang/cổng thông tin điện tử của các cơ quan, tổ chức được sử dụng để cung cấp thông tin đến người dân, doanh nghiệp, bạn bè quốc tế cũng như sử dụng để cung cấp các dịch vụ công trực tuyến luôn phải đối mặt với các nguy cơ tấn công, thay đổi giao diện, cài mã độc trên website…

Cục An toàn thông tin đã xây dựng, phát triển và triển khai Hệ thống phân tích, dò quét, tự động phát hiện tấn công từ xa các website, cổng thông tin điện tử. Hệ thống được thiết kế để hỗ trợ việc theo dõi, giám sát và cảnh báo sớm về mức độ ATTT của các website. Hệ thống thực hiện giám sát từ xa nhưng không can thiệp, không cài đặt phần mềm hay thiết bị vào hạ tầng của các cơ quan chủ quản website đó.

3. Hệ thống theo dõi, phát hiện mã độc, mạng botnet từ xa

Hệ thống theo dõi cập nhật về tình hình mã độc hại được xây dựng và triển khai để hỗ trợ đắc lực trong việc nắm bắt cụ thể và đầy đủ nhất về tình hình lây nhiễm mã độc trong Việt Nam. Từ đó có thông tin để xây dựng kế hoạch và phương án xử lý bóc gỡ các mã độc trên diện rộng.

Với hệ thống này cho phép các cán bộ quản lý, phân tích nắm bắt được chi tiết các dòng mã độc, các mạng botnet đang hoạt động trên không gian mạng Việt Nam.



Bên cạnh đó hệ thống còn giúp các cán bộ phân tích nhanh chóng nắm bắt được xu thế lây lan, phát triển của các họ mã độc, từ đó đề ra các phương án ứng phó kịp thời cho từng thời điểm.

4. Hệ thống giám sát và phòng, chống tấn công mạng

Hệ thống giám sát và phòng, chống tấn công mạng của Cục ATTT được xây dựng trên cơ sở kết hợp giữa giải pháp thương mại và giải pháp nguồn mở, bảo đảm không phụ thuộc vào bất kỳ một hãng hay một công nghệ cụ thể nào trong việc hỗ trợ bảo vệ các hệ thống thông tin.

Cơ quan, tổ chức có thể liên hệ để được tư vấn, hỗ trợ trong công tác bảo đảm ATTT, cụ thể như sau:

- **Đăng ký nhận thông tin cảnh báo chung về ATTT, liên hệ**: Ông Hà Văn Hiệp, số điện thoại: 0968689111, thư điện tử: hvhiep@mic.gov.vn;

- **Đăng ký theo dõi, giám sát trang/cổng thông tin điện tử, liên hệ:** Ông Nguyễn Sơn Tùng, số điện thoại: 0977325416, thư điện tử: nstung@mic.gov.vn;

- **Đăng ký theo dõi, giám sát, xử lý mã độc, lừa đảo qua mạng, liên hệ:** Bà Bùi Thị Huyền, số điện thoại:0932481987; thư điện tử: bt_huyen@mic.gov.vn;

- **Đăng ký hỗ trợ cài đặt cảm biến (sensor) để giám sát, phòng, chống tấn công mạng, liên hệ**: Ông Nguyễn Phú Dũng, số điện thoại: 01676611700, thư điện tử: npdung@mic.gov.vn